




Acceptable Use of ICT Services Policy

Purpose:	The purpose of this Policy is to manage the appropriate use of information, communication and technology services.		
Scope:	This Policy is to be adhered to by all stakeholders which include all staff, directors, managers, workers, parents, students, volunteers, contractors, suppliers and visitors at the College. And may be referred to in this Policy under the general term of 'users' or referenced specifically as required.		
Legislation:	<ul style="list-style-type: none">• <i>Privacy Act 1988 (Cth)</i>• <i>Criminal Code Act 1899 (Qld)</i>• <i>Copyright Act 1968 (Cth)</i>• <i>Australian Cyber Security Centre (ACSC) Guidelines</i>• <i>Queensland Government Enterprise Architecture (QGEA) Guidelines</i>• <i>eSafety Commissioner – Digital Wellbeing</i>		
Ormiston College Related Documents:	<ul style="list-style-type: none">• Anti-Bullying Policy• Anti-Discrimination Policy• Copyright Policy• ICT Personnel Code of Ethics• Personal Electronic Device on Campus Policy• Privacy Policy• Staff Code of Conduct Policy• Student Expectations and Behaviour Code• Cybersecurity Incident Response Plan		
Policy Owner:	College Governing Body	Version:	V100725
Status:	Approved	Supersedes Version:	V190623
Authorised By:	MICHAEL HORNBY	To Be Reviewed:	Every 2 years
Date of Authorisation:	14/7/2025	Next Review Date:	July 2027
Signature:			

Once printed this is an uncontrolled document

POLICY STATEMENT

At Ormiston College, users have the right to utilise ICT Services as essential teaching, learning and business tools. Ormiston College expects this technology to be utilised to its full capacity to provide the most valuable learning and teaching environment to the benefit of all. Ormiston College also expects users to demonstrate acceptable use via safe, lawful and ethical behaviour whenever using ICT Services.

This Policy applies wherever Ormiston College ICT Services are utilised or accessed, whether on the school premises, or outside the College (eg., at home or abroad) with a College owned device or a personal electronic device whilst accessing Ormiston College services or storing Ormiston College data.

Ormiston College reserves the right to restrict user access to ICT Services if acceptable use requirements are not met or are breached. However, restricted access will not disrupt the provision of the educational program within the school. Users should also note that breaches of this Policy may result in disciplinary action by the College or by third parties outside of the College's control (eg., criminal proceedings).

DEFINITIONS

- **ICT** – means information, communication, and technology.
- **ICT Services or College Systems** – includes but is not limited to ICT networks, systems, facilities, and devices, as defined below and includes those owned, leased or otherwise used by the College.
- **ICT Facilities and Devices** – includes but is not limited to computers (including desktops, laptops, netbooks, palm and handheld devices, PDAs, tablets, eBook readers and related devices such as monitors, keyboards and mice), telephones (including mobiles, iPhones and smart phones), removable media (such as USBs, DVDs, Blu-Rays and CDs), radios or other high frequency communication devices (including microphones), television sets, digital or analogue players and records (including DVD, Blu-Ray and video), cameras, photocopiers, facsimile machines, printers (and other imaging equipment such as scanners), Smartboards, projectors and screens, teleconferencing devices.
- **ICT Network and Systems** – electronic networks, internet, email, web mail, social media, fee-based web services, software, servers.
- **Personal Electronic Devices** – includes all types of mobile and smart phones, laptops, tablets, cameras and video recorders, hand-held game devices, music devices, USBs, PDAs, eBook readers, other palm and handheld devices and other equipment, as determined by the College, and not owned by the College.
- **External ICT Service** – services or equipment not owned by the College but may be accessed via the College's ICT Services, includes but not limited to websites, cloud services, publishing websites.
- **Users** – any person who accesses Ormiston College ICT Services (eg staff member, student, parent, external contractors, community members & visitors). In this document, the term 'you' is considered a user and therefore 'you' and 'users' are used interchangeably throughout this Policy.
- **User Credentials** – Usernames, Passwords, ID Cards, FOBs or any other device or information provided by the College to prove a user's electronic identity.
- **Data** – any information and created works that are provided to, created within and stored on College systems, this may include personal and sensitive information as defined by the *Privacy Act*.

Once printed this is an uncontrolled document

RESPONSIBILITIES

College Responsibilities

Ormiston College acknowledges its responsibility to:

- Develop and implement this Policy to ensure the full utilisation of ICT Services as essential teaching, learning and business tools within acceptable use parameters.
- Communicate this Policy to students, parents and employees.
- Keep appropriate records, monitor and report on any issues related to inappropriate ICT Services use.
- Encourage students, parents and employees to contribute to a healthy school culture.

Employee Responsibilities

Ormiston College employees have a responsibility to:

- Uphold the College's Policy on this issue via safe, lawful and ethical use of ICT Services.
- Provide guidance and model appropriate behaviour for use of ICT Services in the classroom.
- Ensure students operate ICT facilities and devices in a safe manner.
- Take reasonable steps to prevent and appropriately respond to any instances of inappropriate use by students accessing ICT Services.

Student Responsibilities

Ormiston College students have a responsibility to:

- Uphold the College's Policy on this issue by ensuring the appropriate use of ICT Services via safe, lawful and ethical behaviour.
- Report any breaches of this Policy to the teacher or the Manager – ICT Services.

Parent/Guardian Responsibilities

Parents/Guardians have a responsibility to:

- Ensure their children understand the College's ICT access and usage requirements, including acceptable and unacceptable behaviour requirements.
- Ensure their children appropriately use internet and technology at home, including when their child is provided a College owned ICT device for study purposes.

External Users and Community Members

External Users and Community Members have a responsibility to:

- Uphold the College's Policy on this issue via safe, lawful and ethical use of ICT Services.
- Report any suspicious activity to the Manager – ICT Services.

Once printed this is an uncontrolled document

WHAT IS ACCEPTABLE USE?

By using Ormiston College ICT Services, users must demonstrate acceptable use via safe, lawful and ethical behaviour.

In summary, examples of Unacceptable Use (as defined by the Queensland Department of Education) include:

Unlawful, Criminal, Offensive or Obscene Material
Uploading, downloading, storing, forwarding or in any way distributing or communicating the following: <ul style="list-style-type: none">• Pornography• Inappropriate pictures, graphics, jokes or messages (particularly any material of sexually explicit, racist, sexist, discriminatory or otherwise potentially offensive behaviour, including the use of inflammatory, obscene, vulgar, insulting, abusive, threatening, harassing or provocative language).• Unlawful or criminal material.• Any other material which is likely to cause offence, or which would be considered socially unacceptable. This includes the presence of the above information (whether accessed or not) on: <ul style="list-style-type: none">• External storage devices connected to the College ICT Services (personal or otherwise).• Personal mobile devices accessing or syncing to College ICT Services.• College owned mobile devices accessing or syncing to College ICT Services.
Defamatory and Fraudulent Material and Use
<ul style="list-style-type: none">• Uploading, downloading, storing, forwarding or in any way distributing or communicating information that is untrue, defamatory, libellous, misleading or deceptive.• Impersonating other people or falsely claiming to represent other people whether alive or dead, real or fictional.• Scanning images of another person's signature and storing or transmitting to other users – whether on purpose or by accident.
Use for Personal Profit or Commercial Purposes
<ul style="list-style-type: none">• Using College ICT Services to conduct personal business for personal gain or profit, including fee-based or subscription services or stock trading.• Uploading, forwarding or communicating any commercial advertising material or any commercial websites for personal gain.
Counterproductive Use and Exploitation of College ICT Services
<ul style="list-style-type: none">• Overseas or other expensive personal phone calls or IP calls (eg., toll numbers).• Downloading and/or playing any inappropriate or time-consuming games or software.• Accessing gambling websites, dating services online.• Accessing filesharing sites online and downloading or using filesharing software applications.• Downloading or storing files and records, including audio or video files in file sharing formats, which are not for officially approved purposes or that were obtained illegally, including using College ICT Services to download to Personal devices.

Once printed this is an uncontrolled document

- Downloading and/or distributing material such as chain letters or letters relating to pyramid schemes.
- Knowingly performing any act which degrades or otherwise negatively impacts the performance of College ICT Services or an external party ICT network (eg., downloading excessively large files or software, use of excessive amounts of bandwidth (eg., audio or video streaming), spamming, transmitting files that may place an unnecessary burden on College ICT Services or external parties.
- Knowingly downloading and/or executing material from the internet, email or external storage device containing viruses, worms, Trojan horses, spyware or any other contaminating or destructive features.
- Creating or maintaining personal websites (except in the course of authorised use for educational purposes).

Political or Religious Advocacy

- Advocating religious or political opinions.
- Participating in any lobbying or political activity or endorsing political parties or candidates.

Violating Privacy and Confidentiality

- Uploading or sharing personal information, including photographs or personal details (such as names, private addresses or telephone numbers) of third parties (including staff, teachers or students) without prior consent.
- Recording an individual whether that be in the form of video or audio without that person's permission or without permission from an authorised member of staff.
- Deliberately forwarding sensitive or confidential College information or documents to webmail or other personal email accounts.
- Intentionally scanning or photographing College documents or information and storing or circulating through unapproved channels.

Breaching Intellectual Property Ownership & Copyright

- Providing a third-party information or material without obtaining the appropriate intellectual property permissions.

Contributing to Public Discussion in a way that is Contrary to the Public Interest

- Using work email addresses when creating personal website accounts or profiles.
- Making comments or disclosures concerning your official roles and duties (this includes disclosing work-related information, documents, images, etc.) or work-related activities and events unless the information is in the public domain.
- Citing or referencing the College's students, parents, partners, suppliers or employees without prior approval, except where such information is in the public domain.
- Engaging in attacks or insults of any kind including:
 - online arguments or flame wars by participating in repeated hostile and insulting interactions with other users of websites or forums.
 - trolling behaviour by posting inflammatory, extraneous or off-topic comments on websites or forums with the primary intent of provoking other users of the website.
 - cyber-bulling, cyber-stalking or cyber-harassment by posting content with the intention to torment, threaten, intimidate, humiliate, embarrass or otherwise target other users of websites or forums.
- Engaging in any other action which could harm the goodwill or reputation of Ormiston College.

Once printed this is an uncontrolled document

DIGITAL WELLBEING AND MENTAL HEALTH

Users of College systems, whether at the College or off campus should observe safe practices whilst using ICTs, these include:

- Ensuring your posture is sufficient for the type of device you are using.
- Taking regular breaks from the screen.
- Avoid 'doomscrolling' (the act of spending an excessive amount of time reading large quantities of news, particularly negative news, on the web and social media) and think critically about what you see online.
- Verify who you are talking with in online interactions.
- Be aware of online fraud and scams. Be particularly cautious where the exchange of identity documents or finances are involved in an online dealing.
- Report illegal, restricted content & online abuse to the Manager – ICT Services.

MAINTAINING SECURITY ONLINE

When given access to Ormiston College ICT systems you become a custodian of the data and information that you can access on these systems. Some of this data may be personal or sensitive information about students, parents and others, which **must be used** in compliance with the Australian Privacy Laws. Other data is subject to copyright and distribution laws, in other cases it is intellectual property that is owned by the College and thus must not be redistributed without authorisation. The College is also required by federal law to ensure unauthorised access to content is mitigated by ensuring best practice procedures when using College ICT Services. Should personal or sensitive information become leaked to the public, the College may be forced, by the *Privacy Act*, to notify the government and those who's information was leaked, and you and the College may be subject to a Government audit.

Furthermore, the College has a Cyber Security Response Plan in place that is enacted and followed in the instance of a cyber security attack or data breach.

For more information, please refer to Ormiston College's Privacy Policy.

To Protect College Personal and Sensitive Information

You must not:

- Remove protection software on College devices, including virus scanners, spam filters.
- Alter information or College data without authority to do so.
- Share user credentials (eg., usernames and password), including personal and others that may be given to carry out work with other people.
- Share another person's personal information including names, addresses, phone numbers, photos, credit card details, over email or internet without first obtaining approval from the Manager – ICT Services.
- Attempt to gain access to information above or outside of authorised access level.
- Attempt to disguise the identity or origin of a message, downloaded material or other material of another person, or disguising own identity when sending such material.

Once printed this is an uncontrolled document

You must ensure:

- Passwords are not easily guessable by others. Passwords should have a combination of letters, numbers and characters where possible to strengthen security.
- The discovery of another person's password is immediately reported to the ICT Helpdesk.
- Reasonable precautions are taken to protect school information and systems against unauthorised access, illegal or unauthorised use, disclosure, modification, duplication, disruption or destruction.
- Seek approval from the Manager – ICT Services before downloading or purchasing software or using a Cloud service or website requiring personal information.
- There is active supervision of students and internet use in the classroom, in particular the use of online Chat Rooms and other messaging and communications software.

More specifically, to maintain security online, you should also:

- Report suspicious emails to the ICT Helpdesk, and don't open attachments or links unless advised it is safe to do so.
- Avoid sending Financial, Medical or Personal Information via email, as it is not secure. Generally, there should be a secure transfer option provided by the College or the other party. Seek advice from the ICT Helpdesk before proceeding.
- Ensure the computer is locked when away from it and not in use.
- Keep physical paperwork on workspace secure and hidden from prying eyes.
- Avoid storing data on portable media but if necessary, keep USBs, CDs, DVDs and other portable storage media secure.
- When communicating with parents and the community, follow the Marketing Department's Communication Guidelines, use the Staff Kiosk Communication System where possible, or the BCC field for multiple email recipients if unable to use the Staff Kiosk Communication System. Ensure the email recipient knows the email is for their eyes only.
- In the case of losing College ICT devices, or College information/email is on personal devices that is lost or stolen, notify the Manager – ICT Services as soon as possible so remedial action can be taken.
- Report to the Manager – ICT Services as soon as possible any suspicion that personal information may have been accidentally lost or leaked somehow to the public.
- Report to the Manager – ICT Services as soon as possible if any physical User Credentials, including ID Card, FOBs or physical electronic authentication tokens have been lost.
- Report to the Manager – ICT Services as soon as possible any situation where a cyber threat or ransom has been made against yourself or the College.

CONTENT AND INTELLECTUAL PROPERTY

The use of content online is subject to various conditions, both under the Australian Copyright Law, International Copyright Law, signed contracts and agreements as well as licenses that the College pays annually to cover the use of certain content.

Once printed this is an uncontrolled document

You must not:

- Use College ICT Services to copy and redistribute content that is not owned by you and where you do not have the authority to do so.
- Plagiarise or modify content to make it appear as your own.
- Use photocopiers to make copies of copyrighted material that is not allowed to be copied.
- Make copies of DVDs, CD's, Blu-Ray's where you have to break the encryption mechanism, built into the disc in order to make a copy.
- Publish the original work of another person at the College or the College's intellectual property, marketing and branding without permission.

Distribution of Intellectual Property covered by License:

Generally, most content that is covered by a license to distribute (eg., APRA, AMCOS) contains its own restrictions that is outlined in the License. Online, electronic distribution of this content for educational reasons may be allowed, but it generally is on the condition that it is still kept secure by a username and password. For example, uploading into Microsoft Teams, as opposed to a publicly facing website. You should check with the Manager – ICT Services, before proceeding to upload content outside of the on-premises ICT network and systems.

MAINTAINING ELECTRONIC RECORDS

By law, the College must retain certain information and depending on the type of information, this may have to be kept for up to 99 years. Examples of such information include but are not limited to Student Enrolment records, Academic, Attendance, Financial, Governance or Board related, Health, Custodial, Correspondence with external parties or parents, Consent or Permission, Agreements and Contracts.

To comply, the College has internal procedures for the storing and archiving of records both physical and electronic. More information can be obtained from the Business Manager.

In terms of Electronic records:

- The appropriate portal, management tool or network storage location must be used to store data appropriately to meet the retention requirement. This may mean making copies of data to store in these locations. For example, storing permission slips in TASS, downloading documentation from cloud services such as Office 365 OneNote and storing locally on S-Drive.
- Information that should be retained must not be deleted. Ask the Manager – ICT Services before deleting information.
- Do not attempt to correct or alter historical data stored on College ICT Services without first seeking authorisation from the Manager – ICT Services.

ICT PHYSICAL RESOURCES

The College expects appropriate care is taken for all ICT equipment and services, and to not use the equipment in any way that is considered unsafe, dangerous, or could disrupt the ICT Services of another person. In addition to this, Students and Parents must agree to a Laptop Agreement if issued an Ormiston College laptop that can be taken home.

Once printed this is an uncontrolled document

You must not:

- Move a fixed ICT device, asset or resource from its location without permission from ICT Services (eg., moving a phone handset, printer, or other equipment determined to be in a fixed location eg., Maker Space, VR, Science Lab etc).
- Wilfully cause damage to any ICT device or resource owned by the College.
- Reverse engineer or change the inner workings of a device so that it becomes dangerous or is no longer fit for purpose.
- Deliberately waste ICT resources (eg., printing).
- Leave devices in an unworkable state where it can be reasonably avoided by user intervention (eg., photocopiers or printers left without paper, stuck on a print job and not cancelled, user serviceable paper jam). Notify ICT Services for assistance.
- Deliberately book out or use too many ICT facilities or devices in surplus to needs, at the cost of access for other users.
- Fail to return a borrowed ICT item within a reasonable time after its due date to be returned.

You must:

- Report all damage to ICT equipment immediately to the ICT Helpdesk.
- Report immediately to the ICT Helpdesk when an Item has been lost or stolen.
- Operate all ICT equipment within the operating instructions of the device and as instructed in Ormiston College ICT Professional Development or documentation.
- Report immediately to ICT Helpdesk if it is suspected an ICT device has become unsafe. Remove people from using the device and turnoff where safe to do so. If the device has caught on fire and the fire is spreading, immediately follow the College's evacuation procedures.
- A College owned device or ICT resource must not be taken off campus unless authorised to do so or have signed a Laptop Agreement authorising to take the device home. Seek authorisation from the Manager – ICT Services.
- Return any College supplied ICT equipment at the cessation of employment or enrolment at the College.

EMERGING TECHNOLOGIES & SHADOW ICTs

To ensure the safe use of ICTs as well as being compliant with State and Federal laws, the College must regulate the use of ICTs. To do so, the College supplies ICTs equipment and services that have been well vetted within the education community and creates practices for its own community of users to follow for the protection of all.

New technologies and emerging technologies often come with no ability to be corporately managed or with guarantees on cyber security and data protection. For example, Artificial Intelligence through their terms and conditions may require a user to accept conditions that severely waiver the rights of the user and the College.

- Users must not purposely use 3rd party equipment or services without the specific approval of the Manager – ICT Services.
- Users must consult with the Manager – ICT Services and seek approval prior to signing up to new ICT services including cloud services.
- Users must not copy College owned data onto 3rd party, privately owned ICT devices or systems.

Once printed this is an uncontrolled document

PERSONAL USE OF COLLEGE ICT RESOURCES

The College recognises there will be times that College ICT Services are used for personal reasons. The College expects this use to be minimal and in line with this Acceptable Use of ICT Services Policy and the College's Social Media Policy.

The College does not expect ICT Resources to be used to advance a person's personal business, commercial interest or to advocate or lobby for certain political views. If there is a conflict of interest where using the College ICT Resources results in a personal gain or prosperity, the College does not endorse the use of its ICT Services.

Acceptable personal reasons for using College ICT Resources include:

- Internet banking & paying bills
- Internet shopping
- Checking personal email
- Recreational use, movies, music, games (as long as the content is within the bounds of this Acceptable Use of ICT Services Policy).

Personal use should not be during work time, eg., use during breaks, before or after hours.

Users should avoid the storage and distribution of personal or sensitive information via College ICT Resources, as this information could be potentially compromised in the event of a Cyber Security incident.

College user credentials or email addresses should not be used as a contact point for any personal dealings with other businesses or external ICT Services.

PERSONAL DEVICES

The College allows limited use of personal devices whilst on Campus. In general, both students and staff must seek permission from the Manager – ICT Services prior to using personal devices on the College campus. There is a Personal Electronic Devices on Campus Policy that students and staff must also comply with.

When using personal devices at home to access College ICT Services online, the rules in this Acceptable Use of ICT Services Policy, the College Privacy Policy and the College Social Media Policy apply.

ACCESSIBILITY AND INCLUSION

The College will ensure users who have specific disabilities, medical conditions or diverse learning needs will be able to access College ICT systems and devices. The College considers needs on a case-by-case basis and includes the following elements:

- Support of the use of personal assistive devices on campus.
- Procurement of specialist equipment and software to improve accessibility.
- Compliance within the College's Workplace Health and Safety Policy to ensure safe access to College ICT systems.

Users are encouraged to contact the ICT Services Helpdesk should they have trouble accessing ICT Services.

Once printed this is an uncontrolled document

MONITORING ICT USE

By law, the College must monitor the use of ICT Services within the College. This includes emails and any information that passes through the College ICT network and systems regardless if it is personal/private information or not.

The College must respond to any requests for information from authorities, court subpoenas and in some cases freedom of information requests. These requests may include all available information on a particular person or persons. In addition to documents, files and other data that the user stores on College ICT systems, the College will collect and store:

- Login records, device use
- Logs of what has been modified or changed
- A log of sites a user accessed over the internet
- Records of internet chat, messaging and other conversations
- Emails
- Electronic ID Card use, including locations accessed in the College by Electronic Card
- Information on what is printed or copied
- Security Camera footage around the College grounds
- Phone Call Data (Note: actual phone conversations are only recorded if all parties on the call are notified. By default, the College does not record phone conversations).

The College is allowed to:

- Seize College owned ICT devices from students, staff or others who use College ICT equipment at its own discretion.
- Seize personal devices used at the College, if it reasonably believes the devices are being used in breach of this and other agreements.
- Use the College provided user credentials for a particular user to access resources.
- Revoke at any time, user credentials such as usernames, access cards and ICT equipment without giving reason.

WHO HAS ACCESS TO THIS INFORMATION?

For Students

A formal request can be made in writing to the Manager of ICT Services by:

- **A teacher** – If the request relates to disruption in a classroom or investigating off-task behaviour of an individual student.
- **A member of College Executive** – Where the matter involves damage, multiple students, cheating, bullying and abuse or other matters, a member of College Executive would reasonably investigate within their role.

For Other Reasons

A formal request for access can only be made by the **Headmaster** or **Deputy Head of College**. Staff, parents and other users should first send a request for information to the Headmaster or Deputy Head of College.

Once printed this is an uncontrolled document

Board of Directors

As per Director's responsibilities governing the Ormiston College entity and associated entities, by authority and due process, the Chairman of the Board of Directors may formally request access to stored information on College ICT systems.

ICT Services

As ICT personnel are the architects of ICT Systems, key members of the ICT Services Department have the potential to access personal information. Upon employment, each member of the ICT Services Department agrees to the ICT Personnel Code of Ethics Policy. This document outlines how a member must conduct themselves ethically when working with personal and sensitive information. There are serious consequences for a member of the ICT Services Department who does not abide by this Policy.

CONSEQUENCES FOR USERS

Consequences for breaching this Acceptable Use of ICT Services Policy are as follows:

- Detention, exclusion and possible termination of enrolment
- Termination of employment
- Exclusion from the College Community
- Prosecution in an Australian Court of Law
- Civil action by other members of society.

Once printed this is an uncontrolled document

TEXT FOR STUDENT HANDBOOK

ACCEPTABLE USE OF ICT SERVICES

All students at Ormiston College have the right to utilise ICT Services as essential learning tools, to assist in the undertaking of studies such to achieve valuable and meaningful learning outcomes.

Ormiston College expects students to demonstrate acceptable use via safe, lawful and ethical behaviour whenever using ICT Services. Parents and Guardians should ensure their children understand and adhere to the conditions outlined in the wider Acceptable Use of ICT Services Policy, Social Media Policy and Privacy Policy, all available in Student Café and Parent Lounge.

To assist students with understanding of their obligations, below is a summary from these Policies.

Whether being on campus under the care of Ormiston College, or at home under the care of Parents and Guardians, when using College ICT Services, students must not:

- Access, download, distribute, or publish material that is unlawful, illegal, unsafe, or unethical.
- Author and send, or resend, offensive, obscene, abusive, messages, videos, music, pictures or other material that is considered socially unacceptable.
- Use ICT Services to be insulting, harassing, bullying or attacking in behaviour to another person or student.
- Share their College username and password or use another person's username and password to access College ICT Services and/or external ICT Services without the College's approval to do so.
- Share their ID Card with another student or use another student's ID Card without the College's approval to do so.
- Use Cloud services, internet chat, social media, play games or other unauthorised software in the classroom without permission from the teacher and, where applicable, permission from your Parent/Guardian.
- Record a person (audio/video) or take photographs of a person without their permission or without permission from a member of staff.
- Make publicly available, another person's personal information including names, addresses, phone numbers, photos, financial and medical details, or any other information considered personal or sensitive under the *Australian Privacy Act*. Students should be guided by the teacher or Parent/Guardian on what is appropriate even if the student has the person's consent to share their information.
- Attempt to gain access to information that you are not authorised to have.
- Wilfully cause damage to any ICT device or ICT resource owned by the College.
- Reverse engineer or change the inner workings of a device so that it becomes dangerous to themselves or others or it becomes no longer fit for purpose.

Once printed this is an uncontrolled document

- Reverse engineer or bypass software that is designed to monitor or control the use of ICT facilities or devices or attempt to bypass College mechanisms it provides to keep learning on task and to ensure safe use of technology.
- Purposely cause disruption to the College ICT systems and network; whether that be by installing inappropriate software (eg., viruses, hacking tools), making use of services on the internet to attack the College or threaten its online security (eg., DDOS Attack), or misusing College ICT Services in a way that impacts the access of ICT Services for others (eg., Excessive Downloads or printing).
- Fail to return a loaned ICT item within a reasonable time frame after its due date to be returned.
- Use personal ICT equipment within the College campus that has not been approved by the Manager – ICT Services.

INFORMATION FOR PARENTS

The College will monitor all student activity on its ICT Systems, and will, where required, inspect emails, files, College assigned laptops and other College owned devices students may use at its discretion. This includes whilst on campus, but also remotely when required.

The College has a Duty of Care for the safe use of College ICT Systems and has in place Internet filters and Security software for College ICT Systems on campus and laptop devices taken home by students. Whilst the filtering software used by the College is considered 'Enterprise Class' and is adopted by other Colleges in the region, by nature of the complexity involved in providing a safe internet service, on rare occasions, filtering cannot always prevent illicit content from appearing on a student's screen.

Likewise, some students, as part of their own behaviour, may choose to deliberately break the conditions of the Acceptable Use of ICT Services Policy and share inappropriate or illicit content with other students. The College does not condone these actions, and upon becoming aware of such circumstances will investigate vigorously with appropriate consequences applied.

Students who are the victim of any inappropriate or illicit behaviour that is contrary to the Acceptable Use of ICT Services Policy, or see content that is inappropriate, must report this to the classroom teacher or the ICT Helpdesk immediately.

In addition, the College also, as part of its duty of care provides workshops, training and other online resources for students and parents on Cyber Safety and the safe use of technology. Parents are strongly advised to make use of these resources as they continue to work with their child(ren) on appropriate online behaviour.

CONSEQUENCES

For students who break the Acceptable Use of ICT Services Policy, consequences include:

- Weekly Monitoring or Supervision
- Detention
- Withdrawal of ICT Services eg., Email
- Suspension or Expulsion
- Involvement of Law Enforcement and other external agencies.

Once printed this is an uncontrolled document

CLASSROOM PLACARD FOR JUNIOR SCHOOL

Using Laptops in classrooms

- I must ask permission from my classroom teacher to use a laptop.
- I must ensure I secure the laptop in the trolley when not in use.
- I must plug the laptop into the charger in the trolley.
- I must carry the laptop with the lid shut.
- I must report all damage to my classroom teacher immediately.

Security & Privacy

- I will not share my password with anyone else.
- I will not attempt to use or interfere with another student's laptop, or password.
- I will not reveal any of my own or another person's private information on the internet (eg., personal address, phone number, banking information).
- I will not use online chat, social media, messaging programs or other email addresses except for what is provided by the College and where my classroom teacher allows me to.

Appropriate Use

- I must not use the College's laptop or internet to access, download or distribute material that is unlawful, illegal, unsafe or unethical. This includes pirated material.
- I will not use the laptop to offend or bully another student.
- Any data stored on the laptop, including emails and attachments are subject to routine inspection by the College.

Consequences

- Weekly monitoring or supervision.
- Detention.
- Withdrawal of ICT Services eg., email.
- Supervision or Expulsion.
- Involvement of law enforcement and other external agencies.

Once printed this is an uncontrolled document